

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347944

(43)Date of publication of application : 15.12.2000

(51)Int.Cl.

G06F 12/14

(21)Application number : 11-159486

(71)Applicant : SHARP CORP

(22)Date of filing : 07.06.1999

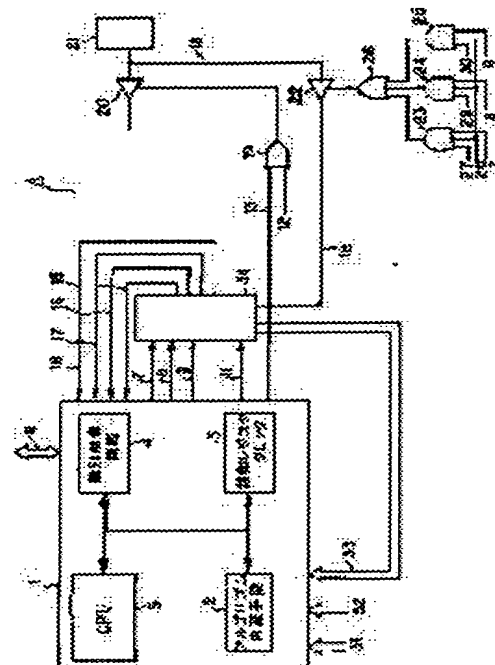
(72)Inventor : HAYASHI HIROTAKE

## (54) MICROCOMPUTER WITH BUILT-IN NONVOLATILE MEMORY

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a one-chip microcomputer with a built-in nonvolatile memory capable of performing security protection of data with a simple operation.

**SOLUTION:** This microcomputer is provided with a dedicated security flash memory 14 which automatically stores the last data to be written in an internal flash memory 21 as a security code, a controller 1 controlling an access to the memory 21, an OR circuit 19 and a tri-state buffer 20. After the data writing to the memory 21 is finished, the controller 1, etc., is allowed to access the memory 21 only when data coinciding with a security code is inputted externally.



## LEGAL STATUS

[Date of request for examination]

18.01.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

**BEST AVAILABLE COPY**

Copyright (C); 1998,2003 Japan Patent Office

## 引用例 3 の写し

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-347944

(P2000-347944A)

(43) 公開日 平成12年12月15日(2000.12.15)

(51) Int.Cl.

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

テーマコード(参考)

3 2 0 C 5 B 0 1 7

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願平11-159486

(22) 出願日 平成11年6月7日(1999.6.7)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 林 裕 ▲ 丈 ▼

大阪府大阪市阿倍野区長池町22番22号

シャープ株式会社内

(74) 代理人 100112335

弁理士 藤本 英介

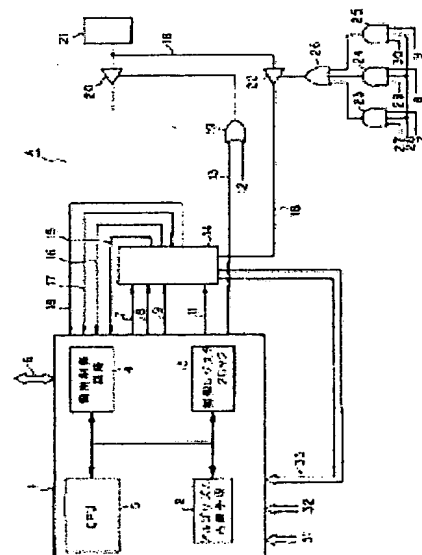
Fターム(参考) 5B017 AA01 BA05 CA13

(54) 【発明の名称】 不揮発性メモリ内蔵マイクロコンピュータ

(57) 【要約】

【課題】 簡単な操作によってデータの機密保持が可能な不揮発性メモリ内蔵 1チップマイクロコンピュータを提供すること。

【解決手段】 内蔵フラッシュメモリ21へ書き込まれる最終データをセキュリティコードとして自動的に記憶するセキュリティ専用フラッシュメモリ14と、内蔵フラッシュメモリ21へのアクセスを制御する制御装置1、OR回路19、およびトライステートバッファ20とを設け、制御装置1等は、内蔵フラッシュメモリ21へのデータの書き込み終了後においては、セキュリティコードと一致するデータが外部から入力された場合にのみ内蔵フラッシュメモリ21へのアクセスを可能とする。



【特許請求の範囲】

【請求項 1】 不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリへのアクセスを制御する制御手段とを設け、前記制御手段は、前記不揮発性メモリへのデータの書き込み終了後においては、前記セキュリティコードと一致するデータが外部から入力された場合に不揮発性メモリへのアクセスを可能とすることを特徴とする不揮発性メモリ内蔵マイクロコンピュータ。

【請求項 2】 不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリに対するアクセスを制御するアルゴリズムを内蔵したアルゴリズム内蔵手段と、前記セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後に、前記アルゴリズム内蔵手段の制御の下で、前記不揮発性メモリへのアクセスを禁止するアクセス禁止手段と、を設けたことを特徴とする不揮発性メモリ内蔵マイクロコンピュータ。

【請求項 3】 前記アクセス禁止手段は、前記アルゴリズム内蔵手段に格納されたアルゴリズムで無限ループを実行することで不揮発性メモリへのアクセスを禁止することを特徴とする請求項 2 に記載の不揮発性メモリ内蔵マイクロコンピュータ。

【請求項 4】 前記セキュリティコードと一致するデータを外部より入力することにより、前記アクセス禁止手段による不揮発性メモリへのアクセス禁止状態を解除することを特徴とする請求項 2 又は 3 に記載の不揮発性メモリ内蔵マイクロコンピュータ。

【請求項 5】 不揮発性メモリへのアクセスを可能、或いは不揮発性メモリへのアクセス禁止状態を解除した後、セキュリティコードと一致しないデータを外部より入力することにより再度不揮発性メモリへのアクセスを禁止することを特徴とする請求項 1 又は 4 に記載の不揮発性メモリ内蔵マイクロコンピュータ。

【請求項 6】 前記セキュリティコードは、不揮発性メモリへ書き込まれる最終データであることを特徴とする請求項 1 又は 2 に記載の不揮発性メモリ内蔵マイクロコンピュータ。

保護に関する。

【0002】

【従来の技術】 従来、不揮発性メモリ（例えばフラッシュメモリ）の内蔵された 1 チップマイクロコンピュータでは、内蔵不揮発性メモリへのアクセス、すなわちデータ書き込み、読み出し、データ消去を行う際、後述の 3 種の動作モードが用意され、各モード毎に専用ボードが使用される。これらの動作モードを実現する概略的な構成は内蔵不揮発性メモリにアクセスするアルゴリズムを内蔵している不揮発性のプログラムメモリ、CPU 及び内蔵不揮発性メモリアクセス動作に関連する識別制御回路、制御レジスタ等からなる。

【0003】 これらのモードには、(1) PROM ライターによる専用アダプタを使用しデータの書き込み、消去、読み出しの行える PROM モード、(2) 外部メモリ (PROM 等) から専用ボードを使用してフラッシュメモリへデータのコピーを行うコピーモード、(3) 製品のプリント基板に実装されたフラッシュメモリーの内蔵された 1 チップマイクロコンピュータデバイスに対してシリアルポートを介してデータを書き込むシリアル転送モード（以下、オンボードモードという）がある。そこで、これらの各モードでメモリデータの機密保持を行う必要がある場合、それを実現するための機能を各モード毎に備えていなければならない。

【0004】 従来、本機能を実現するために以下のようなものがある。

(a) PROM ライターによるデータの読み出しを行う際、予め入力されたセキュリティコードが不揮発性メモリへ記憶されており、このセキュリティコードに対するコードを外部端子等で入力し、一致しない限り読み出し禁止とする。あるいは、書き込みを行う際、特定の端子等を設定することで、PROM ライターでの再度の書き込み及び読み出しを不可能とする。このようにして、メモリデータ機密保持を図る。

【0005】 (b) コピーモードによる書き込みも前記 (a) 同様予め入力されたセキュリティコードが不揮発性メモリへ記憶されており、このセキュリティコードに対するコードを外部端子等で入力し一致しない限り読み出しが禁止になりメモリデータの保護が行われる。

【0006】 (c) オンボードモードでは、所定のフォーマットに従ってプログラムにパスワードを予め設定しユーザプログラム書き込み時に同一のパスワードを入力しない限りアクセスされないことで保護される。

【0007】 上記のように本来のデータアクセス以外に予め、セキュリティコードあるいはパスワードを設定する必要がある。

【0008】 図 2 に、従来技術の一例による不揮発性メモリを内蔵した 1 チップマイクロコンピュータのデータメモリ保護に対する概略的な構成例を示す。これは、特開平 5-73428 に開示されている技術を簡略に示し

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、マイクロコンピュータに内蔵される不揮発性メモリのメモリデータを読み出し装置から読み出し不可能とするようなメモリデータ

たものである。不揮発性メモリが内蔵されたメモリデータを読み出し禁止とする方法として、セキュリティコード記憶不揮発性メモリ100へ予めコードを記憶させ、入力キーコードラッチ回路101でセキュリティコード記憶不揮発性メモリ100へ記憶させたコードと同一コードを入力する。この情報は比較回路102で判断され一致している場合のみ読み出し制御部103へ一致信号が出力されて、比較結果用不揮発性メモリ104からの比較結果信号105と、図示しないCPUからのリード信号106とでメモリ108を読み出し可能とする。イーナブル信号107が出力されることで、メモリ108から図示しない内部データバス或いは、外部の端子へデータの読み出しが行われる。

【0009】

【発明が解決しようとする課題】しかしながら、従来の方法では予めセキュリティコードを不揮発性メモリへ設定し、このセキュリティコードに対するコードを外部より入力しなければならず、メモリデータへの書き込みを行う操作以外の設定による作業が必要になると同時に、セキュリティコードを改めて規定するためにその管理が煩雑となっていた。

【0010】本発明は、前記の問題点を解消するためなされたものであって、簡単な操作によってデータの機密保持が可能な不揮発性メモリ内蔵1チップマイクロコンピュータを提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は、上記の目的を達成するため、次の構成を有する。本発明の第1の要旨は、不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリへのアクセスを制御する制御手段とを設け、前記制御手段は、前記不揮発性メモリへのデータの書き込み終了後においては、前記セキュリティコードと一致するデータが外部から入力された場合に不揮発性メモリへのアクセスを可能とすることを特徴とする不揮発性メモリ内蔵マイクロコンピュータである。

【0012】また、本発明の第2の要旨は、不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリに対するアクセスを制御するアルゴリズムを内蔵したアルゴリズム内蔵手段と、前記セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後に、前記アルゴリズム内蔵手段の制御の下で、前記不揮発性メモリへのアクセスを禁止するアクセス禁止手段と、を設けたことを特徴とする不揮発性メモリ内蔵マイクロコンピュータである。

【0013】さらに、本発明の第3の要旨は、前記アク

セス禁止手段は、前記アルゴリズム内蔵手段に格納されたアルゴリズムで無限ループを実行することで不揮発性メモリへのアクセスを禁止することを特徴とする要旨2に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【0014】また、本発明の第4の要旨は、前記セキュリティコードと一致するデータを外部より入力することにより、前記アクセス禁止手段による不揮発性メモリへのアクセス禁止状態を解除することを持つとする要旨2又は3に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【0015】また、本発明の第5の要旨は、不揮発性メモリへのアクセスを可能、或いは不揮発性メモリへのアクセス禁止状態を解除とした後に、セキュリティコードと一致しないデータを外部より入力することにより再度不揮発性メモリへのアクセスを禁止することを持つとする要旨1又は4に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【0016】さらにまた、本発明の第6の要旨は、前記セキュリティコードは、不揮発性メモリへ書き込まれる最終データであることを特徴とする要旨1又は2に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【0017】要旨1によれば、不揮発性メモリへデータが書き込まれると同時に、或いは書き込まれた後に、セキュリティ専用不揮発性メモリにそのデータの一部がセキュリティコードとして自動的に記憶される。セキュリティコードは所定ルールに基づきくものであるため、データを書き込んだ者は知り得るが、他人には知れ得ないこととなる。そして、その不揮発性メモリへのデータへの書き込みが終了した後は、セキュリティコードと一致するデータが外部から入力されないかぎり、制御手段が不揮発性メモリへの再度のアクセスを不可とするので、他人による書き込み動作、読み出し動作、消去動作等のアクセスが不可となり、不揮発性メモリ内のデータの機密保持が可能となる。従来、不揮発性メモリ内のデータの機密保持を行なう場合には、不揮発性メモリへデータの書き込み操作と別個にセキュリティコードの入力操作を行っていたが、本発明ではセキュリティコードの入力操作が不要となるのと同時に、改めてセキュリティコードを用意する必要もなくなるので簡単な手段にて機密保持が可能となった。

【0018】また、要旨2によれば、不揮発性メモリへデータが書き込まれると同時に、或いは書き込まれた後に、セキュリティ専用不揮発性メモリにそのデータの一部がセキュリティコードとして自動的に記憶される。そして、セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後は、アルゴリズム内蔵手段の制御の下で、アクセス禁止手段が不揮発性メモリへの再度の書き込み動作、読み出し動作、消去動作等のアクセスを禁止するので、他人によるアクセスが不可となり、不揮

発性メモリ内のデータの機密保持が可能となる。従来、不揮発性メモリ内のデータの機密保持を行なう場合には、不揮発性メモリヘデータの書き込み操作と別個にセキュリティコードの入力操作を行なっていたが、本発明ではセキュリティコードの入力操作が不要となるのと同時に、改めてセキュリティコードを用意する必要もなくなるので簡単な手段にて機密保持が可能となった。

【0019】また、要旨3によれば、アクセス禁止手段がアルゴリズム内蔵手段に格納されたアルゴリズムで無限ループを実行することで、アクセス待ち状態（データ書き込み動作、消去動作、読み出し動作のいずれかに相当するルーチン待ち）が無く、見かけ上アクセス不能状態となる。すなわち、デバイス自体が内蔵メモリをアクセスできない故障あるいは不良の状態と同等となるため、実質的に他者によるメモリデータの読み出しは困難でありメモリ内容のセキュリティが保たれる。

【0020】さらにまた、要旨4によれば、セキュリティコードは所定ルールに基づくものでありデータを書き込んだ者は知り得るので、不揮発性メモリ内のデータの修正等を行なう場合にはセキュリティコードと一致するデータを外部より入力することにより可能となる。

【0021】また、要旨5によれば、不揮発性メモリ内のデータの修正等を行った後に、セキュリティコードと一致しないデータを外部より入力するという簡単な操作により再度不揮発性メモリへのアクセスを禁止することが可能となり、簡単な操作により修正が可能となる。

【0022】さらに、要旨6によれば、セキュリティコードを不揮発性メモリへ書き込まれる最終データとすることで、セキュリティコード等の設定が簡単な回路により実現することができる。

【0023】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。図1は、マイクロコンピュータであって、より具体的にはプロセッサと共にメモリ、例えばフラッシュメモリを1チップに集積、内蔵した1チップマイクロコンピュータAの主要部位のブロック図を示している。1は内蔵フラッシュメモリ21へのアクセスを行う制御装置であり、14は制御装置1から内蔵フラッシュメモリ21へのアクセスを制御するためのセキュリティ専用フラッシュメモリ14である。

【0024】制御装置1には、PROMモード、コピーモード、オンボードモードの各モードを認識し、書き込み動作、読み出し動作、及び消去動作の各プログラムを内蔵しているアルゴリズム内蔵手段2と、そのアルゴリズム内蔵手段2内のプログラムが実行されて内蔵フラッシュメモリ21をアクセスする際の制御レジスタブロック3と、PROMモード時のPROMライタコマンド等に対する識別制御を行う識別制御回路4と、これらの制御をつかさどるCPU5とを有する概略構成とし、各モードによる動作を可能とする。尚、制御装置1の各種入

出力信号については、後述する。

【0025】内蔵フラッシュメモリ21には、図示しない各種出力端子との間に制御スイッチであるトライステートバッファ20が接続され、内蔵フラッシュメモリ21からのデータ出力がコントロールされるとともに、内蔵フラッシュメモリ21とセキュリティ専用フラッシュメモリ14との間にもトライステートバッファ22が設けられ、セキュリティ専用フラッシュメモリ14のデータ出力も制御されている。

【0026】前記トライステートバッファ20のオンオフをコントロールするコントロールゲートは、制御装置1等からの信号を入力信号とするOR回路19の出力端子に接続され、結果的に制御装置1からの信号13や後述する信号12によりそのON/OFF制御が成されている。また、トライステートバッファ22のコントロールゲートには各モード（PROMモード、コピーモード、オンボードモード）毎に対応して設けられたAND回路23、24、および25の出力信号を入力信号とするOR回路26の出力端子が接続され、各モード毎のセキュリティ専用フラッシュメモリ14へのデータの出力を制御している。

【0027】次に、各モードによるセキュリティの動作を説明する。まずPROMモードの動作時における制御装置1では、PROMライタインターフェイス信号6を介して図示しないPROMライタとのアクセスを可能にする数種類の信号が入出力し、識別制御回路4でPROMライタからのコマンド、データ、制御データの認識を行い、データ書き込みコマンドに対する処理が実行される。これにより、内蔵フラッシュメモリ21へのPROMモードでのデータの書き込みがなされる。

【0028】そして、最終のデータ書き込みサイクル期間、制御装置1よりPROMモード書き込み終了信号7にライト信号28パルス出力に対し、セットアップ、ホールド期間を保持してHighを出力させる。このとき同時に最終のデータ書き込みサイクル期間、PROMモード書き込み終了信号7はPROMモード用のAND回路23へも入力される。

【0029】PROMモード用のAND回路23の残り2入力信号は、PROMモード信号27とライト信号28であり、PROMモード信号27は現在PROM書き込みモードであるのでHighとなり、またライト信号28は最終書き込みデータ期間のみHighパルスが有効となる。以上より、AND回路23はHighを出力する。

【0030】そしてPROMモード用のAND回路23の出力信号は、トライステートバッファ22のコントロールゲートを制御するOR回路26へ入力される。尚、前記OR回路26は、各モードに対応して3入力信号となっており、残り2入力の信号はコピーモード用のAND回路24の出力信号とオンボードモード用のAND回

路25の出力信号が入力される。

【0031】現在PROM書き込みモードの状態であるために、コピーモード用のAND回路24の入力信号であるコピーモード信号29と、オンボードモード用のAND回路25の入力信号であるオンボードモード信号30は共に非アクティブであるのでOR回路26へはLow信号が入力される。よって、OR回路26の入力は、PROMモード時のAND回路23の出力信号が有効となってトライステートバッファ22のコントロールゲートへ入力され、最終書き込みデータ期間のみゲートが開き、セキュリティ専用フラッシュメモリ14へのデータ出力が可能となる。

【0032】これにより内蔵フラッシュメモリ21からの最終書き込みデータ（ここでは、例として8ビット長のデータを示す）をセキュリティ専用フラッシュメモリ14に、セキュリティコードとして書き込み、PROMモード書き込み終了信号7と共に設定される。

【0033】そして、セキュリティ専用フラッシュメモリ14はPROMモードに対するセキュリティが設定されたことを認識し、PROMモードセキュリティ信号15を出力し、この信号15を受けて、制御装置1内にあるアルゴリズム内蔵手段2内のプログラムで強制的に無限ループループへ起動を掛ける。この起動により制御装置1より無限ループフラグ信号13にLowが出力される。この信号13は、OR回路19へ入力される。また、OR回路19による残りの入力信号である実動作モード信号12は、ユーザプログラムが起動する時の信号であり、このPROMモード時にはLow信号である。

【0034】これらのLow信号12、13が入力されるOR回路19は、Low信号が出力されトライステートバッファ20のコントロールゲートへ入力され、トライステートバッファ20の出力はこのコントロールゲートへの入力信号がHighの時のみインネブルとなることからフローティング状態になり、かつ、制御装置1内にあるアルゴリズム内蔵手段2内で実行中のプログラムがPROMモード動作に対する待機状態でないので、内蔵フラッシュメモリ21のデータをPROMライタから読み出すことが不可能となると同時にPROMライタからの制御そのものも受け付けなくなる。

【0035】また、このPROMモードで書き込まれたメモリ内容は、コピーモードあるいはオンボードモードで読みだそうとしてもPROMモードによる無限ループフラグ信号13を解除しない限り、読み出せない。尚、無限ループフラグ信号13を解除し、メモリ内容を読みだし可能とする手段については後述する。

【0036】次に、コピーモード時はPROMモード同様、最終のデータ書き込みサイクル期間、制御装置1よりコピーモード書き込み終了信号8にライト信号28パルス出力に対し、セットアップ、ホールド期間を保持してHighを出力させる。このとき、コピーモード書き

込み終了信号8は、AND回路24へ入力される。残り2入力のコピーモード信号29は、現在コピーモード書き込みであるのでHigh信号が入力され、ライト信号28は最終書き込みデータ期間のみHighパルスが有効となり、結果的にAND回路24からOR回路26へHighが入力される。

【0037】このOR回路26の残り2入力の信号は、AND回路23の出力とAND回路25の出力であるが、AND回路23の入力にはPROMモード信号27が入力されており、現在コピーモード書き込みの状態であるため両AND回路の出力信号はLowとなっている。従って、OR回路26の入力はコピーモード時のAND回路24の出力信号が有効となりトライステートバッファ22のコントロールゲートへ入力されてゲートが開き、データが出力される。これにより内蔵フラッシュメモリ21から最終書き込みデータ期間のデータをセキュリティ専用フラッシュメモリ14に、セキュリティコードとして書き込み、コピーモード書き込み終了信号8と共に設定される。

【0038】そして、セキュリティ専用フラッシュメモリ14はコピーモードに対するセキュリティが設定されたことを認識し、コピーモードセキュリティ信号16を出力し、この信号16を受けて、制御装置1内にあるアルゴリズム内蔵手段2内のプログラムで強制的に無限ループループへ起動を掛ける。この起動により制御装置1より無限ループフラグ信号13にLowが出力される。この信号13は、OR回路19へ入力される。

【0039】OR回路19の前記した他方の入力信号である実動作モード信号12は、ユーザプログラムが起動する時の信号であり、このコピーモード時にはLow信号である。よって、OR回路19から出力されるLow信号がトライステートバッファ20のコントロールゲートへ入力されてフローティング状態になり、かつ、制御装置1内にあるアルゴリズム内蔵手段2内で実行中のプログラムがコピーモード動作に対する待機状態でないので、内蔵フラッシュメモリ21のデータをコピーモードボードから読み出すことが不可能となると同時にコピーモードボードの制御そのものも受け付けなくなってしまう。

【0040】残り、オンボードモード時も前記したPROMモード、コピーモード時と同様に、最終のデータ書き込みサイクル期間、制御装置1よりオンボードモード書き込み終了信号9にライト信号28パルス出力に対し、セットアップ、ホールド期間を保持してHighを出力させる。以後、前記したモードと同様に最終のデータ書き込みサイクル期間だけ、トライステートバッファ22のコントロールゲートが開き、内蔵フラッシュメモリ21からのデータをセキュリティ専用フラッシュメモリ14に、セキュリティコードとして書き込み、オンボードモード書き込み終了信号9と共に設定される。

【0041】そして、セキュリティ専用フラッシュメモリ14はオンボードモードに対するセキュリティが設定されたことを認識し、オンボードモードセキュリティ信号17を出力し、この信号を受けて、制御装置1内にあるアルゴリズム 内蔵 手段2内のプログラムで強制的に無限ループルーチンへ起動を掛ける。この起動により制御装置1より無限ループフラグ信号13にLowが出力される。

【0042】このLow信号13はOR回路19へ入力され、残りの入力信号の実動作モード信号13もオンボードモード時にはLow信号であるので、OR回路19はLow信号を出力し、トライステートバッファ20はフローティング状態になる。制御装置1内にあるアルゴリズム 内蔵 手段2内で実行中のプログラムがオンボードモード動作に対する待機状態でないで、内蔵フラッシュメモリ21のデータをオンボードモードボードから読み出すことが不可能となると同時にオンボードモードの制御そのものも受け付けなくなる。

【0043】以上説明したような各モードによるメモリデータ内容の読み出し禁止状態を唯一解除する動作として、テストモード信号31とセキュリティコード入力信号32を特定端子に割り当て必要信号を入力するテストモードが用意されている。

【0044】ここでセキュリティコード入力信号32には、セキュリティ専用フラッシュメモリ14へ書き込んだ最終データ（例えば、8ビットデータ長であれば、8本の入力端子の設定）を設定する必要がある。この場合、データ入力を行ったオペレータは最終データを理解していることからセキュリティコード入力信号32への入力をミスなく行うことができ、他人は最終データを知り得ないことからセキュリティコードとして機能する。

【0045】この様に入力条件が満たされたテストモード状態は、アルゴリズム 内蔵 手段2内のプログラムでセキュリティ専用フラッシュメモリ記憶手段14に設定されているデータコード33と該当するテストモード条件の一致が認識されたときのみ、テストモード一致信号11にHighを出力する。

【0046】このテストモード一致信号11で、セキュリティ専用フラッシュメモリ記憶手段14の一致信号18に対するビットがHighにセットされる。一致信号18にHighが出力されることで、アルゴリズム 内蔵 手段2内のプログラムはこの一致信号18を認識して各モード時における無限ループルーチンの制御を各モードに該当するセキュリティの設定されていないデータ書き込み動作、消去動作、及び読み出し動作のいずれかに相当するルーチン待ちの状態へ移行させる。この動作と連動して無限ループフラグ信号13は、LowからHigh信号となることで、OR回路19による出力信号はHighとなり、トライステートバッファ20のコントロールゲートがアクティブとなるので内蔵メモリデータの

内容が読み出し可能となる。

【0047】また、前述の3つの動作モードにおいて、新たに内蔵フラッシュメモリ21に書き込みあるいは消去を行うことも可能となり、内蔵フラッシュメモリ21に格納されているプログラムやデータのメンテナンスが可能となる。

【0048】尚、このテストモードによる読み出しを前述の3つのモードと同様に読み出し禁止とするためには、該当するテストモード状態とセキュリティコード入力信号32をフラッシュメモリの最終データと一致しない信号を入力することで、各モード時のセキュリティ動作で説明したプロセス、すなわちを無限ループフラグ信号13をアクティブにすることで同様なセキュリティが可能となる。

【0049】なお、前記の実施形態では本発明の好適例を説明したが、本発明はこれに限定されないことはもちろんである。例えば、本発明におけるセキュリティコードは、従来のように予めセキュリティコードを入力するのではなく、入力データから所定規則に基づいてセキュリティコードが自動的に作成されるものであればよく、本実施形態では最終のデータをセキュリティコードとして用いる場合を説明したが、例えば、入力データの最初のデータや、所定ルールに基づくデータを用いてもよく、適宜回路を変更することで同様の作用効果を発揮する。また、本実施形態では、説明の便宜上1チップマイクロコンピュータを例に発明を説明したが、1チップに限定するものでないことは言うまでもない。

【0050】

【発明の効果】以上説明した通り、本発明の第1、2の要旨によれば、予めセキュリティコードやパスワードを設定することなく自動的に内蔵フラッシュメモリの読み出し等を禁止でき、かつ、改めてセキュリティコードを用意する必要もなくなるのでセキュリティコード管理も不要となり、簡単に不揮発性メモリ内のデータの秘密保持が可能となった。

【0051】要旨3によれば、アクセス禁止手段がアルゴリズム 内蔵 手段に格納されたアルゴリズムで無限ループを実行することで、アクセス待ち状態がなくなり、見かけ上デバイス自体が内蔵メモリをアクセスできない故障あるいは不良の状態と同等となるため、実質的に他者によるメモリデータの読み出しは困難でありメモリ内容のセキュリティが保たれる。

【0052】要旨4によれば、セキュリティコードは所定ルールに基づくものであり、データを書き込んだ者は知り得ることから、不揮発性メモリ内のデータの修正等を行なう場合にはセキュリティコードと一致するデータを外部より入力することにより、プログラムのバグ発生に伴うメンテナンスを可能とできた。

【0053】要旨5によれば、不揮発性メモリ内のデータ、例えばプログラムのバグ発生に伴うメンテナンス

後、再度セキュリティを簡単にかけることも可能となるので、セキュリティとプログラムやバグ等によるメンテナンス等が確実にできる。

【0054】要旨6によれば、セキュリティコードを不揮発性メモリへ書き込まれる最終データとすることで、セキュリティコード等の設定が簡単な回路により実現することができる。

# 【図面の簡単な説明】

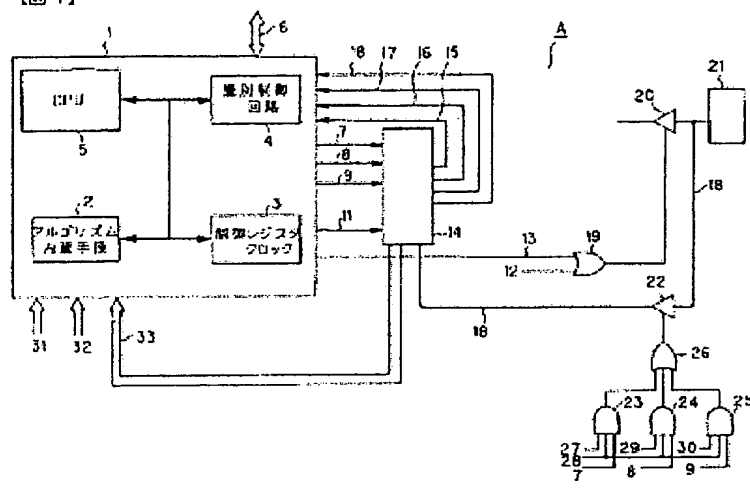
【図1】本発明の実施形態に係る不揮発性メモリ内蔵1チップマイクロコンピュータの概略的ブロック図である。

【図2】従来の不揮発性メモリ内蔵1チップマイクロコンピュータの作用的ブロックである。

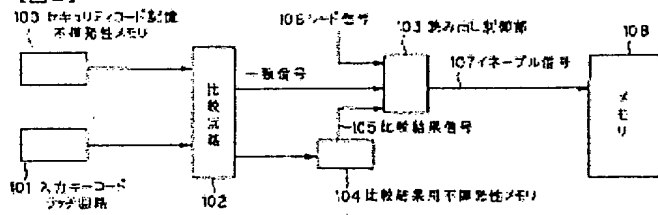
## 【符号の説明】

- A 1チップマイクロコンピュータ
- 1 制御装置
- 2 アルゴリズム内蔵手段
- 14 セキュリティ専用フラッシュメモリ
- 19 OR回路
- 20 トライステートバッファ
- 21 内蔵フラッシュメモリ

【図1】



【図2】





**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**